Math 357
Exam 01

2024–03–01 (F)

Your name: _____

Honor pledge:

Instructions

1. In the space above, please legibly write your name and the Rice Honor Pledge, then sign.
2. Full time for this exam is exactly 50 minutes. No resources are allowed.
3. Your reasoning—correctness and clarity—is more important than your "answer".
4. If you think there is ambiguity or error in an exercise, then briefly (!) write your understanding of the exercise and any additional hypotheses you are making, then proceed.

This exam is an imperfect measure of my understanding at a particular point in time. It is not a measure of who I am or who I will be.

Exercise	Total	(a)	(b)	(c)	(d)
1	/4	/4	/4	/4	
2	/4				
3	/4	/4	/4	/4	/4
4	/4				
5	/4	/4	/4		
Total	/20				

Exercise 1

(4 pt) Let R be a commutative ring with a multiplicative identity $1 \neq 0$. An element $a \in R$ is **nilpotent** if there exists an $n \in \mathbf{Z}_{>0}$ such that $a^n = 0$.

(a) Let $a \in R$ be nonzero. Prove that if a is nilpotent, then a is a zero divisor.

(b) Give an example to show that the converse of (a) is false.

(c) Let $a \in R$ be nilpotent. Prove that $1 - a$ is a unit.

Solution: Part (a): Let $a \in R$ be a nonzero nilpotent element, and let

$$n_0 = \min\{n \in \mathbf{Z}_{>0} \mid a^n = 0\}$$

By hypothesis, (i) a is nilpotent, so this set is nonempty, and hence n_0 is well defined (and exists by the well ordering of $\mathbf{Z}$); and (ii) a is nonzero, so $n_0 \geqslant 2$. Let $b = a^{n_0-1}$. Then $b \neq 0$, and

$$ab = aa^{n_0-1} = a^{n_0} = 0$$

so a is a zero divisor.

Remark. The definition of zero divisor requires only one of $ab = 0$ or $ba = 0$. In the current setting, we get both, because R is commutative.

Part (b): The converse of (a) is the statement, "Let $a \in R$ be nonzero. If a is a zero divisor, then a is nilpotent." To see that this is false, consider the element $a = 2$ in the ring $R = \mathbf{Z}/(6)$. 2 is a zero divisor: $2 \times 3 = 0$. However, 2 is not nilpotent: For all $n \in \mathbf{Z}_{>0}$, $6 \nmid 2^n$ in $\mathbf{Z}$, hence $2^n \neq 0$ in $\mathbf{Z}/(6)$.

Part (c): Let $n_0 \in \mathbf{Z}_{>0}$ be defined as in our solution to part (a), and let

$$b = 1 + a + \ldots + a^{n_0-1}$$

Then[1]

$$(1-a)b = (1-a)(1 + a + \ldots + a^{n_0-1}) = 1 - a + a - \ldots - a^{n_0-1} + a^{n_0-1} - a^{n_0} = 1 - a^{n_0} = 1$$

By hypothesis, R is commutative, so $b(1-a) = 1$ as well. Hence $1 - a \in R^\times$, as desired.

Remarks.

1. In part (a) we assumed that $a \neq 0$. However, our definition of n_0 there is valid for $a = 0$ as well, as is the argument here.
2. In fact, we don't need to take n_0, the minimum positive integer n such that $a^n = 0$. Any such n works for this argument.

[1] In the first equality, we use the definition of b; in the second, the ring axioms, namely, the left distribution law and associativity of $+$; in the fourth, the hypothesis that a is nilpotent and the definition of n_0.

Exercise 2

(4 pt) Let R be an integral domain. Prove that if R is a euclidean domain, then R is a principal ideal domain. (Heart points: Give—without proof—an example of a principal ideal domain that is not a euclidean domain.)

Solution: Remark. The key idea in this proof is that, in a euclidean domain, any nonzero ideal is generated by a nonzero element of minimal norm. The key tool is the division algorithm.

Let R be a euclidean domain, and let $I \trianglelefteq R$ be an ideal. Case 1: $I = (0)$. Then I is principal, and we are done. Case 2: $I \neq (0)$. Then there exist nonzero elements of I. Let b be a nonzero element of I of minimal norm.[2] We claim that $I = (b)$. To see this, let $a \in I$ be arbitrary. By hypothesis, R is a euclidean domain, so there exists a norm N on R with respect to which R has a division algorithm. In particular, $b \neq 0$ by definition, so there exist $q, r \in R$ such that

$$a = bq + r \tag{1}$$

with $r = 0$ or $N(r) < N(b)$. Suppose for the sake of contradiction that $r \neq 0$. Then the conclusion of the division algorithm implies that $N(r) < N(b)$. By the axioms of an ideal, $r = a - bq \in I$, so r is a nonzero element of I of smaller norm than b, contradicting the definition of b. Thus $r = 0$, so equation (1) becomes $a = bq$, and thus $a \in (b)$, as desired. This shows that $I \subseteq (b)$.

The reverse inclusion follows immediately from the definition of an ideal: $b \in I$ if and only if $(b) \subseteq (I) = I$. Hence $I = (b)$, as desired.

The ring $\mathbf{Z}[(1 + \sqrt{-19})/2]$ is a principal ideal domain but not a euclidean domain.[3]

[2] This minimum exists by well ordering of $\mathbf{Z}$: By definition, the image of a norm map is a nonempty subset of $\mathbf{Z}_{\geqslant 0}$.

[3] See Expositional Homework 01.

Exercise 3

(4 pt) For each of the following polynomials, state whether it is reducible or irreducible in the indicated polynomial ring. Justify your assertions.

$$f_1 = t^2 + 2 \in \mathbf{F}_7[t] \qquad f_3 = 6t^4 + 24t^3 + 18t + 81 \in \mathbf{Q}[t]$$
$$f_2 = 4t^3 + 9t^2 + 7t - 12 \in \mathbf{Z}[t] \qquad f_4 = t^4 - 42t^2 + 30t + 12 \in \mathbf{Q}[t]$$

Solution: Remark. One of the beautiful aspects of mathematics is that there are different ways to prove a given statement. Try realizing this beauty here.

Analysis of f_1. Because $\deg f_1 = 2$, f_1 is reducible if and only if the polynomial $f_1 \in \mathbf{F}_7[t]$ has a factor of degree 1, if and only if the function $f_1 : \mathbf{F}_7 \to \mathbf{F}_7$ has a zero. We compute

$$f_1(\pm 3) = -3 \qquad f_1(\pm 2) = -1 \qquad f_1(\pm 1) = 3 \qquad f_1(0) = 2$$

none of which are 0. Thus f_1 is irreducible in $\mathbf{F}_7[t]$.

Analysis of f_2. One approach is to view $f_2 \in \mathbf{Q}[t]$. Then, because $\deg f_2 = 3$, the polynomial $f_2 \in \mathbf{Q}[t]$ is reducible if and only if the function $f_2 : \mathbf{Q} \to \mathbf{Q}$ has a zero.[4] By the rational zeros theorem, we know that if $\frac{a}{b}$ is a zero of f_2, then a divides the constant term of f_2 and b divides the leading coefficient of f_2.[5] Thus,

$$a \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\} \qquad b \in \{\pm 1, \pm 2, \pm 4\}$$

If we just look at the number of elements in each set, then we estimate $(2 \cdot 6) \cdot (2 \cdot 3) = 72$ possible values for $\frac{a}{b}$. We can reduce this number by half, by observing that only the sign of the "combined" fraction $\frac{a}{b}$, not the signs of a and b separately, matter. We can reduce the number a little more by omitting repeated values (for example, $\frac{1}{1} = \frac{2}{2} = \frac{4}{4}$). This leaves about thirty possible values for $\frac{a}{b}$—quick for a computer, too many for me. Can we do even better?

We can reduce this number significantly by viewing $f_2 \in \mathbf{R}[t]$. Note that

$$f_2(0) = -12 < 0 \qquad f_2(1) = 8 > 0$$

Because polynomials with real coefficients define continuous functions $\mathbf{R} \to \mathbf{R}$, the intermediate value theorem implies that f_2 has a zero in the interval $(0, 1)$. Assuming this is the only interval on which f_2 has real zeros (see Remark 2.2 below), this leaves only three values of $\frac{a}{b}$ consistent with the divisibility conditions, namely, $\frac{1}{4}, \frac{1}{2}, \frac{3}{4}$.

If we're willing to invest a little more work up front, we can do even better. We compute

$$f_2\left(\frac{1}{2}\right) = 4 \cdot \frac{1}{8} + 9 \cdot \frac{1}{4} + 7 \cdot \frac{1}{2} - 12 < 1 + 3 + 4 - 12 = -4 < 0$$

so the zero of f_2 must be in the interval $(\frac{1}{2}, 1)$. This implies that the only possible rational zero of f_2 is $\frac{3}{4}$. We compute

$$f_2\left(\frac{3}{4}\right) = \frac{27}{16} + \frac{81}{16} + \frac{84}{16} - \frac{14^2 - 2^2}{16} = 0$$

[4] Why does this logic not work for $f_2 \in \mathbf{Z}[t]$?

[5] succinctly, $a \mid f_2(0)$ and $b \mid \mathrm{LC}(f_2)$.

Thus f_2 is reducible in $\mathbf{Q}[t]$.

We're not done yet—the exercise asks us whether f_2 is reducible in $\mathbf{Z}[t]$. Gauß's lemma states that if f_2 is reducible in $\mathbf{Q}[t]$, then it's reducible in $\mathbf{Q}[t]$. OK, now we're done. For fun, let's see how Gauß's lemma unfolds in this concrete example. We found that $\frac{3}{4}$ is a (rational) zero of f_2, or equivalently, that $t - \frac{3}{4}$ is a factor of f_2 in $\mathbf{Q}[t]$. The explicit factorization (which we can get from polynomial division) is

$$f_2 = \left(t - \frac{3}{4}\right)\left(4t^2 + 12t + 16\right)$$

Gauß's lemma appears as the fact that we can take a constant factor out of the second polynomial and distribute it through the first in such a way that both polynomials end up in $\mathbf{Z}[t]$. Here, that constant factor is 4, and the result is

$$f_2 = (4t - 3)(t^2 + 3t + 4)$$

witnessing the claim that f_2 is reducible in $\mathbf{Z}[t]$.

Remark 2.1. Because f_2 is reducible (although we don't know this, a priori), if we reduce f_2 modulo any prime $p \in \mathbf{Z}$ that does not divide the leading coefficient (why do we make this restriction?), then we'll find that the residue $\bar{f}_2 \in (\mathbf{Z}/(p))[t]$ is reducible (that is, factors into two or more factors of positive degree). If we reduce modulo a few primes and find that $\bar{f}_2$ always factors, then we might suspect (though not be guaranteed!—remember the example from class) that these factorizations are "shadows" of an "original factorization" of f_2.

Moreover, if so, then the "shadow" factorizations provide clues about the factorization of f_2. Consider reducing f_2 modulo the first few "valid" primes:[6]

$$\begin{aligned}
&\mathbf{Z}/(3) : \bar{f}_2 = t^3 + t = t(t^2 + 1)\\
&\mathbf{Z}/(5) : \bar{f}_2 = -t^3 - t^2 + 2t - 2 = (-t + 2)(t^2 - 2t - 1)\\
&\mathbf{Z}/(7) : \bar{f}_2 = -3t^3 + 2t^2 + 2 = (-3t - 3)(t^2 + 3t - 3)
\end{aligned}$$

From these data, we might conjecture that $f_2 \in \mathbf{Z}[t]$ factors into a factor of degree 1 (necessarily irreducible) and an irreducible factor of degree 2; and that the factor of degree 1, denote it $bt + a$, satisfies the relations

$$b \equiv 1 \bmod 3, b \equiv -1 \bmod 5, b \equiv -3 \bmod 7 \qquad a \equiv 0 \bmod 3, a \equiv 2 \bmod 5, a \equiv -3 \bmod 7$$

From these equivalences, we might conjecture that $b = 4$ and $a = -3$.[7] We can then check whether $(4t - 3) \mid f_2$ or, equivalently (why?), whether $f_2(\frac{3}{4}) = 0$.

Question: The reduction technique applies to all ideals, not just prime ideals, that do not contain the leading coefficient. So why do we restrict our preceding analysis to prime ideals?[8] In fact, we don't have to restrict to prime ideals, but we do have to ignore certain nonprime ideals (which?). Before we know the value of b, we won't know which to ignore.

[6] A priori, we don't know with which factors to put negative signs, if there are any. Note that this matters (why?).

[7] Claim: If we use primes p that are large enough—for which we can give an upper bound of p such that $\lfloor \frac{p}{2} \rfloor$ is greater than or equal to the largest coefficient of the original polynomial in $\mathbf{Z}[t]$—then the representatives stabilize to the actual coefficients of the factors.

[8] Hint: denominators.

Remark 2.2. In fact, though our argument does not need it (why not?), we can prove this is so, invoking calculus one more time.[9] Again viewing f_2 as a function $f_2 : \mathbf{R} \to \mathbf{R}$, we compute its first derivative to be

$$f_2'(t) = 12t^2 + 18t + 7$$

I claim this function is always positive. We can see this in various ways:

1. The discriminant of f_2' is $18^2 - 4(12)(7) = 324 - 336 < 0$. Thus the function f_2' has no real zeros. Because f_2' is a polynomial, the function f_2' is continuous. Because $f_2'(0) = 7 > 0$, it follows that for all $t \in \mathbf{R}$, $f_2'(t) > 0$.

2. Completing the square, we find

$$f_2' = 12\left(t^2 + \frac{3}{2}t - \frac{9}{16}\right) + 7 + 12\left(\frac{9}{16}\right) = 12\left(t + \frac{3}{4}\right)^2 + \alpha$$

   where $\alpha = 7 + \frac{27}{4} = \frac{55}{4} > 0$. The exact value doesn't matter; what matters is that $\alpha > 0$. Because the square of any real number is nonnegative, it follows that for all $t \in \mathbf{R}$, $f_2'(t) > 0$.

This says that f_2 is monotonically increasing. From the function's end behavior, we conclude that f_2 has exactly one real zero.

Analysis of f_3. Note that $\deg f_3 = 4$, so checking for zeros of the function f_3 is not sufficient to determine irreducibility. Two irreducibility detectors that do apply to this situation are reduction modulo an ideal and its corollary, the Eisenstein–Schöonemann criterion.

Using the Eistenstein–Schönemann criterion: View $f_3 \in \mathbf{Z}[t]$. The only prime that divides the constant term of f_3 is 3. Note that 3^2 also divides the constant term, so we cannot apply the Eisenstein–Schönemann criterion directly to f_3. However, recall[10] that a polynomial with nonzero constant term is irreducible if and only if its reverse is irreducible. The reverse of f_3 is

$$\operatorname{rev} f_3 = 81t^4 + 18t^3 + 24t + 6$$

To this polynomial, we may apply the generalized statement of the Eisenstein–Schönemann criterion[11] with $p = 2$: $p = 2$ does not divide the leading coefficient, it does divide all other coefficients, and $p^2 = 4$ does not divide the constant term. Thus, by the criterion, $\operatorname{rev} f_3$ is irreducible in $\operatorname{Frac}(\mathbf{Z})[t] = \mathbf{Q}[t]$, which as we have noted is equivalent to the statement f_3 is irreducible in $\mathbf{Q}[t]$.

Using reduction modulo an ideal: View $f_3 \in \mathbf{Z}[t]$. The reduction technique requires that we do not send the leading coefficient of the polynomial to zero, so the smallest prime we may use with f_3 is $p = 5$.[12] Reducing the coefficients of f_3 modulo 5, we get

$$\bar{f}_3 = t^4 - t^3 - 2t + 1$$

The function associated to this polynomial has a zero (in fact, two):

$$\bar{f}_3(-1) = 1 + 1 + 2 + 1 \equiv 0 \qquad \bar{f}_3(2) = 16 - 8 - 4 + 1 \equiv 0$$

[9] Calculus in algebra? Why not?!

[10] See Expositional Homework 03, from DF3e, Exercise 9.5.16, p 312.

[11] See Expositional Homework 03, from DF3e, Exercise 9.5.17, p 312.

[12] What happens if we reduce the coefficients modulo 4?

This decides nothing. Remember the shadows principle: Under suitable hypotheses (for example, that the polynomial be nonconstant and monic), a factorization in $R[t]$ will appear as a factorization in $(R/I)[t]$ for every proper ideal $I \lhd R$. However, an irreducible polynomial in $R[t]$ may have reducible reductions in some (sometimes all!) nonzero quotients $(R/I)[t]$.

The next ideal we can try is $(7) \trianglelefteq \mathbf{Z}$. In this case, we get

$$\bar{f}_3 = -t^4 + 3t^3 - 3t - 3$$

Evaluating the associated function $\bar{f}_3$ at the seven elements of $\mathbf{Z}/(7)$, we find that $\bar{f}_3$ has no zeros.[13] It remains to check that $\bar{f}_3 \in \mathbf{F}_7[t]$ has no factors of degree 2. To certify this, it suffices to check only the monic degree-2 polynomials (why?), of which there are 49; and in fact, to check only the irreducible monic degree-2 polynomials (why?), of which there are 21.[14] This is more polynomial divisions than I'd want to perform by hand in a timed exam environment,[15] so I'd briefly sketch this approach for the grader, then look for others.

Analysis of f_4. Note that $\deg f_4 = 4$, so our introductory comments in our analysis of f_3 also apply here. The only primes that divide the constant term are 2 and 3. Both primes do not divide the leading coefficient and do divide all other coefficients. However, 2^2 divides the constant term, so we cannot use $p = 2$. 3^2 does not divide the constant term. Thus the Eisenstein–Schönemann criterion[16] with $p = 3$ implies that f_4 is irreducible in $\mathbf{Z}[t]$, and Gauß's lemma[17] implies that f_4 is therefore irreducible in $\mathbf{Q}[t]$.

[13] In particular, you—or your favorite computing machine—should find

$$\bar{f}_3(-3) = -2 \qquad \bar{f}_3(-2) = -2 \qquad \bar{f}_3(-1) = 3 \qquad \bar{f}_3(0) = -3 \qquad \bar{f}_3(1) = 3 \qquad \bar{f}_3(2) = -1 \qquad \bar{f}_3(3) = 2$$

[14] In general, let $p \in \mathbf{Z}_{>0}$ be prime, and let $\mathbf{F}_p$ be the finite field with p elements. The number of reducible monic polynomials of degree 2 in $\mathbf{F}_p[t]$ equals the number of ways of choosing, with replacement, two elements from p elements (why?), which equals $\binom{p+2-1}{2} = \frac{(p+1)p}{2}$. Alternatively, we can reason as follows: If a monic degree-2 polynomial in $\mathbf{F}_p[t]$ factors, then it has either two distinct zeros or two identical zeros. The number of possibilities in the first case is $\binom{p}{2}$, and in the second case is p, so the total number is $\frac{p(p-1)}{2} + p = \frac{(p+1)p}{2}$.

To read more on these topics, see Math Stack Exchange posts 1393337 (irreducible polynomials over a finite field) and 474741 (intuition for combinations with replacement).

[15] Or any environment, really.

[16] See DF3e, Proposition 9.13, p 309.

[17] See DF3e, Proposition 9.5, p 303.

Exercise 4

(4 pt) Let F be a field, let $\alpha \in F$, and let t be an indeterminate. We may give $F[t]$ the structure of a ring, an $F[t]$-module, or a $\mathbf{Z}$-module. For each map below, state whether it is a ring homomorphism, an $F[t]$-module homomorphism, or a $\mathbf{Z}$-module homomorphism. Justify your assertions. *Hint:* A given map may satisfy several or none of these conditions. The characterization may depend on the value of α.

$$\begin{aligned} \varphi : F[t] &\to F[t] \\ f(t) &\mapsto \alpha f(t) \end{aligned} \qquad\qquad \begin{aligned} \psi : F[t] &\to F[t] \\ f(t) &\mapsto f(\alpha) \end{aligned}$$

Solution: Recall that a $\mathbf{Z}$-module is equivalent to an abelian group, so a $\mathbf{Z}$-module homomorphism is equivalent to a homomorphism of abelian groups.[18] By definition, given a ring $(R, +, \times)$, $(R, +)$ is an abelian group. In particular, we may view the polynomial ring $F[t]$ as an abelian group if we keep addition and ignore multiplication.

Let $f_1, f_2 \in F[t]$. We compute

$$\varphi(f_1 + f_2) = \alpha(f_1 + f_2) = \alpha f_1 + \alpha f_2 = \varphi(f_1) + \varphi(f_2)$$

where in the second equality we use the left-distributive law in $F[t]$; and

$$\psi(f_1 + f_2) = (f_1 + f_2)(\alpha) = f_1(\alpha) + f_2(\alpha) = \psi(f_1) + \psi(f_2)$$

where in the second equality we use the definition of addition of functions (!). We conclude that both φ and ψ are $\mathbf{Z}$-module homomorphisms.

It remains to analyze how the maps treat multiplication: "external" scalar multiplication and "internal" ring multiplication. Note that the "scalars" in the $F[t]$-module $F[t]$ are polynomials in $F[t]$, and the scalar multiplication is defined by the multiplication in the ring $F[t]$. Let $f, g \in F[t]$.

For φ, we compute

$$\varphi(gf) = \alpha(gf) = g \cdot (\alpha f) = g\varphi(f) \qquad\qquad \varphi(g)\varphi(f) = \alpha g \cdot \alpha f = \alpha^2 gf$$

We conclude that, for all $\alpha \in F$, φ is an $F[t]$-module homomorphism. It is a ring homomorphism if and only

$$\alpha gf = \varphi(gf) = \varphi(g)\varphi(f) = \alpha^2 gf \quad \Leftrightarrow \quad (\alpha^2 - \alpha)gf = 0 \quad \Leftrightarrow \quad \alpha = 0 \text{ or } 1$$

where in the final equivalence we use the fact that $F[t]$ is an integral domain (why?) to invoke the cancellation law. If our definition of a homomorphism of rings with a multiplicative identity requires that the map send the multiplicative identity in the domain to the multiplicative identity of the codomain, then φ is a ring homomorphism if and only if $\alpha = 1$.

For ψ, we compute

$$\psi(gf) = (gf)(\alpha) = g(\alpha)f(\alpha) = \psi(g)\psi(f) \qquad\qquad g\psi(f) = g(t)f(\alpha)$$

We conclude that, for all $\alpha \in F$, ψ is a ring homomorphism.[19] For all $\alpha \in F$, ψ is not an $F[t]$-module homomorphism: It is an $F[t]$-module homomorphism if and only if, for all $g, f \in F[t]$,

$$g(\alpha)f(\alpha) = \psi(gf) = g\psi(f) = g(t)f(\alpha) \quad \Leftrightarrow \quad (g(t) - g(\alpha))f(\alpha) = 0$$

which holds if and only if the ring of coefficients is the zero ring, which by definition a field is not.

[18] See DF3e, p 339 and p 346 Example (4).

[19] The map ψ—usually with its codomain taken to be F, not $F[t]$—is often called evaluation at $t = \alpha$.

Exercise 5

(4 pt) Let F be a field, let G be a finite group, and let V be a unital FG-module.

(a) We have seen that V affords a representation $\rho : G \to GL(V)$. Given $g \in G$, define $\rho(g)$.

(b) Prove that for each $g \in G$, $\rho(g) \in GL(V)$.

Solution: Part (a): Given $g \in G$, we use the ring action on V—that is, the map $\cdot : FG \times V \to V$ that is part of the module axioms—to define the representation ρ. Specifically, for each $g \in G$,

$$\begin{aligned} \rho(g) : V &\to V \\ v &\mapsto (1_F g) \cdot v \end{aligned}$$

Part (b): We verify two properties:

(i) For each $g \in G$, the map $\rho(g)$ is linear.

(ii) For each $g \in G$, the map $\rho(g)$ is invertible.

(i) $\rho(g)$ is linear. Let $\alpha \in F$; let $v_1, v_2 \in V$; and let $g_0 \in G$ denote the identity element of the group G. Note that for each $v \in V$, the element $(\alpha g_0) \cdot v$ in V, viewed as an FG-module, is the same element as $\alpha \cdot v$ in V, viewed as an F-module (aka F-vector space).[20] We compute

$$\begin{aligned} \rho(g)(\alpha \cdot v_1 + v_2) &= (1_F g) \cdot (\alpha \cdot v_1 + v_2) \\ &= (1_F g) \cdot ((\alpha g_0) \cdot v_1) + (1_F g) \cdot v_2 \\ &= ((1_F g)(\alpha g_0)) \cdot v_1 + (1_F g) \cdot v_2 \\ &= (\alpha g) \cdot v_1 + (1_F g) \cdot v_2 \\ &= (\alpha g_0) \cdot (1_F g) \cdot v_1 + (1_F g) \cdot v_2 \\ &= \alpha \cdot \rho(g)(v_1) + \rho(g)(v_2) \end{aligned}$$

This shows that for all $g \in G$, $\rho(g) \in \mathrm{Hom}_F(V, V)$.

(ii) $\rho(g)$ is invertible. Let $g_1, g_2 \in G$. For all $v \in V$,

$$\begin{aligned} \rho(g_1 g_2)(v) &= (1_F g_1 g_2) \cdot v \\ &= (1_F g_1) \cdot (1_F g_2) \cdot v \\ &= \rho(g_1)(\rho(g_2)(v)) \\ &= (\rho(g_1) \circ \rho(g_2))(v) \end{aligned}$$

This shows that ρ is a group homomorphism. In particular, let $g \in G$ be arbitrary; if we let $g_1 = g$ and $g_2 = g^{-1}$, then for all $v \in V$,

$$(\rho(g) \circ \rho(g^{-1}))(v) = \rho(gg^{-1})(v) = \rho(g_0)(v) = (1_F g_0) \cdot v = v = \mathrm{Id}_V(v)$$

where Id_V denotes the identity map on V. Likewise, $\rho(g^{-1}) \circ \rho(g) = \mathrm{Id}_V$. Thus, as maps from V to V, $\rho(g)$ and $\rho(g^{-1})$ are inverses. Combined with (i), this shows that for all $g \in G$, $\rho(g) \in GL(V)$.

[20] The ring action $\cdot : FG \times V \to V$ on V as an FG-module is different from the scalar multiplication (aka field action) $\cdot : F \times V \to V$ on V as an F-vector space. Because the two agree in a natural way, as we argue here, we will use the same symbol to denote both.